Relatório Técnico de Análise de Rede – Lab Segmentação de Rede

Autor: Luccas Correa da Silva

Data: 28 de julho de 2025

Versão: 1.0

1. Sumário Executivo

Foi realizada uma análise de segurança na rede simulada, resultando na identificação de uma **falha crítica na segmentação da rede**. A rede designada para visitantes (guest_net, 10.10.30.0/24) contém, na verdade, toda a infraestrutura de servidores críticos da empresa, incluindo um servidor **LDAP (10.10.30.17) que permite conexões anónimas**, representando um risco **Crítico** de fuga de informação. Em contrapartida, a rede que deveria ser a mais segura (infra_net, 10.10.50.0/24) aloja apenas dispositivos de utilizadores finais. Esta inversão anula o propósito da segmentação e expõe os ativos mais valiosos da organização a ameaças diretas. Recomenda-se uma revisão e reestruturação imediata da arquitetura da rede.

2. Objetivo

Analisar a topologia da rede corporativa simulada para identificar a exposição de serviços, avaliar a eficácia da segmentação de rede existente e mapear os riscos operacionais associados às configurações atuais dos ativos.

3. Escopo

O escopo desta análise está restrito ao ambiente de laboratório Docker fornecido, composto por três sub-redes:

- **corp_net (10.10.10.0/24):** Rede corporativa principal.
- **guest_net (10.10.30.0/24):** Rede para visitantes e dispositivos pessoais.
- **infra_net (10.10.50.0/24):** Rede de infraestrutura com servidores críticos.

A análise foi conduzida a partir do host analyst.

4. Metodologia

Ferramentas Utilizadas:

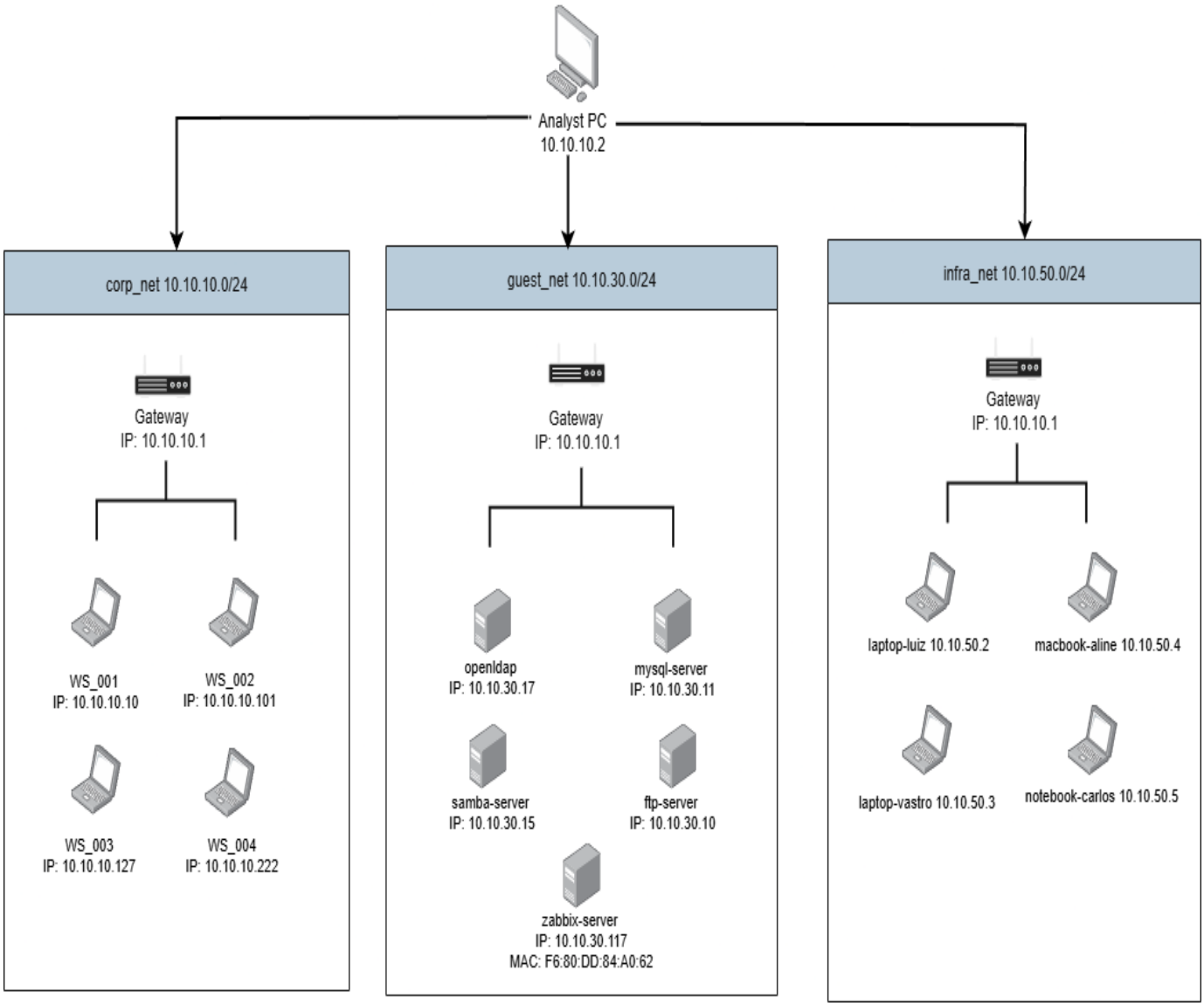
- Net-Tools (ip, ping, curl)

- Nmap (Network Mapper)
- Rustscan
- Utilitários de linha de comando (grep, tee, awk)

Fases da Análise:

- **Fase 1 - Reconhecimento Inicial:** Identificação das interfaces de rede do host de análise e validação da conectividade.
- **Fase 2 - Descoberta de Ativos:** Utilização do Nmap para criar um inventário de todos os hosts ativos em cada sub-rede.
- **Fase 3 - Escaneamento de Portas e Serviços:** Utilização do Rustscan e Nmap (-sV, -sC) para identificar serviços e versões.
- **Fase 4 - Análise Aprofundada e Documentação:** Análise detalhada dos resultados, documentação de cada achado e compilação do inventário de ativos.

5. Diagrama de Rede



6. Inventário de Ativos

A tabela abaixo resume todos os ativos descobertos em cada segmento de rede, com os seus respetivos serviços expostos.

Rede Corporativa (corp_net - 10.10.10.0/24)

IP	Hostname	Portas Abertas	Serviços Identificados	Notas

10.10.10.1	(gateway)	111/tcp, 39881/tcp	rpcbind, status (RPC)	Gateway da rede, expõe serviços RPC.
10.10.10.2	analyst	N/A	(Máquina de análise)	Ponto de partida da análise.
10.10.10.10	WS_001	N/A	(Workstation)	Sem portas abertas detetadas.
10.10.10.101	WS_002	N/A	(Workstation)	Sem portas abertas detetadas.
10.10.10.127	WS_003	N/A	(Workstation)	Sem portas abertas detetadas.
10.10.10.222	WS_004	N/A	(Workstation)	Sem portas abertas detetadas.

Rede de Servidores (guest_net - 10.10.30.0/24) - *Configuração Incorreta*

IP	Hostname	Portas Abertas	Serviços Identificados	Notas
10.10.30.1	(gateway)	111/tcp, 39881/tcp	rpcbind, status (RPC)	Gateway da rede, expõe

				serviços RPC.
10.10.30.10	ftp-server	21/tcp	FTP (Pure-FTPd)	Servidor de ficheiros. Login anónimo desativado.
10.10.30.11	mysql-server	3306/tcp, 33060/tcp	MySQL 8.0.42	Servidor de base de dados. Vaza versão.
10.10.30.15	samba-server	139/tcp, 445/tcp	Samba smbd 4	Servidor de ficheiros. Enumeração anónima desativada.
10.10.30.17	openldap	389/tcp, 636/tcp	OpenLDAP	Servidor de autenticação. **Permite conexão anónima.**
10.10.30.117	Zabbix server	80/tcp, 10051/tcp	HTTP (nginx), Zabbix	Servidor de monitorização. Vaza versão do PHP.

Rede de Utilizadores (infra_net - 10.10.50.0/24) - *Configuração Incorreta*

IP	Hostname	Portas Abertas	Serviços Identificados	Notas
10.10.50.1	(gateway)	111/tcp, 39881/tcp	rpcbind, status (RPC)	Gateway da rede, expõe serviços RPC.
10.10.50.2	laptop-luiz	N/A	Dispositivo de utilizador	Sem portas abertas detetadas.
10.10.50.3	laptop-vastro	N/A	Dispositivo de utilizador	Sem portas abertas detetadas.
10.10.50.4	macbook-aline	N/A	Dispositivo de utilizador	Sem portas abertas detetadas.
10.10.50.5	notebook-carlos	N/A	Dispositivo de utilizador	Sem portas abertas detetadas.

7. Diagnóstico (Achados)

Nesta secção são detalhadas as vulnerabilidades e falhas de configuração identificadas durante a análise, por ordem de criticidade.

Achado 01: Falha Crítica de Segmentação de Rede

- **Risco: Crítico**
- **Descrição:** A análise revelou uma falha grave na arquitetura da rede. A rede que deveria ser a de visitantes (guest_net, 10.10.30.0/24) contém toda a infraestrutura de servidores críticos. Em contrapartida, a rede que deveria ser a de infraestrutura (infra_net, 10.10.50.0/24) contém apenas dispositivos de utilizadores finais.

Achado 02: Fuga de Informação via Conexão Anónima ao Servidor LDAP

- **Host/IP:** 10.10.30.17
- **Risco: Crítico**
- **Descrição:** O servidor LDAP, localizado incorretamente na rede de visitantes, permite conexões anónimas ("anonymous bind").

Achado 03: Servidor de Base de Dados MySQL Exposto com Fuga de Informação

- **Host/IP:** 10.10.30.11
- **Risco: Alto**
- **Descrição:** Um servidor de base de dados MySQL vaza informações detalhadas da versão.

Achado 04: Servidor de Ficheiros Samba/SMB Exposto

- **Host/IP:** 10.10.30.15
- **Risco: Médio**
- **Descrição:** Um servidor Samba está exposto. Testes confirmaram que a enumeração anónima de partilhas está desativada.

Achado 05: Painel de Monitorização Zabbix Exposto com Fuga de Versão de Software

- **Host/IP:** 10.10.30.117
- **Risco: Médio**
- **Descrição:** A interface web de um servidor Zabbix está exposta e divulga a versão exata do PHP.

Achado 06: Divulgação de Serviços RPC através do rpcbind

- **Host/IP:** 10.10.10.1, 10.10.30.1 e 10.10.50.1
- **Risco: Médio**
- **Descrição:** O serviço rpcbind está exposto nos gateways de todas as redes.

8. Recomendações

- **Para o Achado 01 (Segmentação):** Realizar uma reestruturação imediata da arquitetura da rede. Migrar todos os servidores críticos da rede 10.10.30.0/24 para a rede 10.10.50.0/24.
- **Para o Achado 02 (LDAP):** Desativar o "anonymous bind" no servidor OpenLDAP imediatamente.
- **Recomendação Geral:** Após a reestruturação da rede, aplicar regras de firewall rigorosas na rede de infraestrutura (10.10.50.0/24).

9. Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Reestruturar a segmentação da rede (migrar servidores)	**Crítico**	**Baixa**	**Urgente**
Desativar conexão anónima	Crítico	Média	**Crítica**

No LDAP (10.10.30.17)			
Aplicar firewall no MySQL (10.10.30.11)	Alto	Alta	**Alta**
Testar credenciais padrãono Zabbix (10.10.30.117)	Médio	Alta	**Alta**
Aplicar firewall no Samba (10.10.30.15)	Médio	Alta	Média

10. Conclusão

A análise de segurança da rede simulada identificou com sucesso uma **falha arquitetural crítica na sua segmentação**, que é a causa raiz da maioria dos outros riscos encontrados. A colocação de ativos de infraestrutura vitais, como o servidor LDAP, na mesma rede designada para visitantes, anula as políticas de segurança e expõe a organização a um risco inaceitável. É imperativo que a organização priorize a reestruturação da sua topologia de rede, seguida pela correção das vulnerabilidades específicas identificadas.

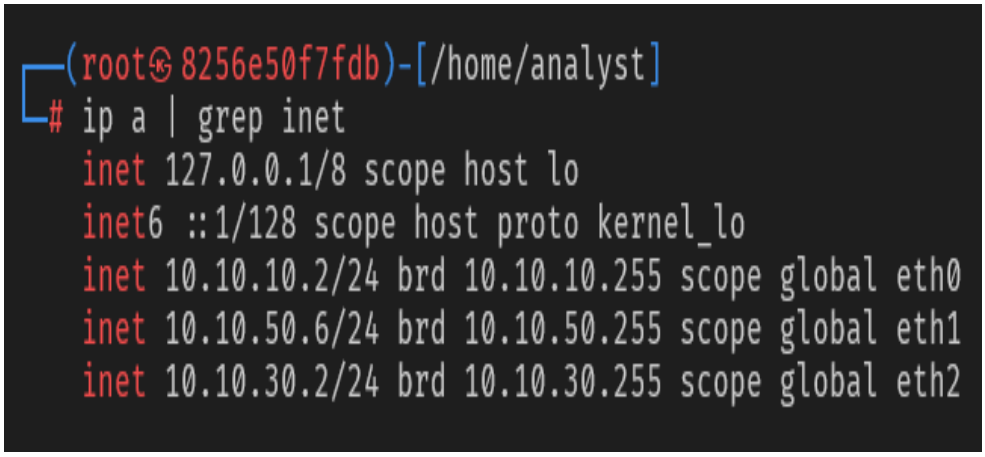
11. Anexos: Guia Completo de Evidências e Análise de Comandos

Esta secção contém as evidências de todos os comandos executados durante a análise, com uma explicação detalhada de cada passo.

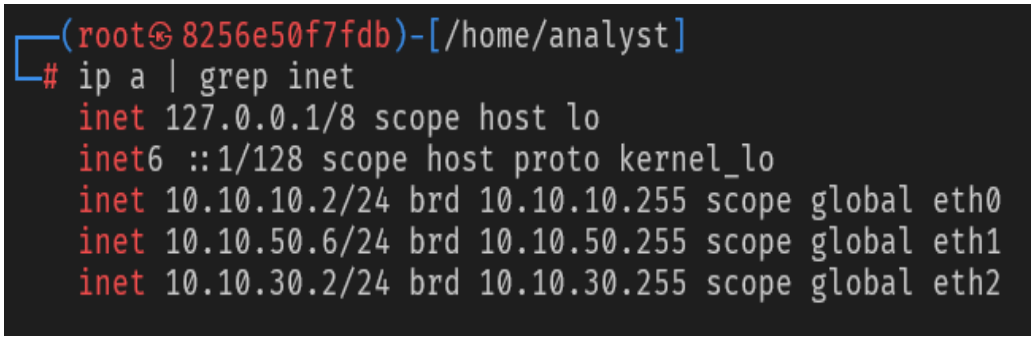
Fase 1: Reconhecimento Inicial

Anexo A: Configuração de Rede do Host de Análise

- **Comando Executado:** ip a
- **Explicação do Comando:** O comando ip a é usado para listar todas as interfaces de rede e os seus respetivos endereços IP. Este é o primeiro passo para entender o nosso ponto de partida.
- Resultado:

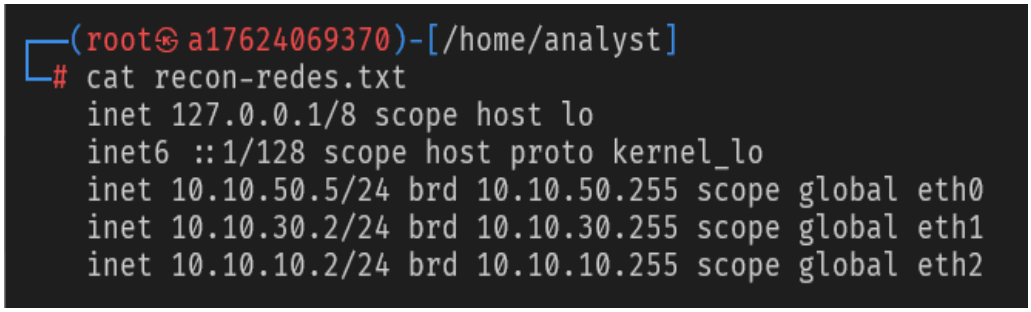


- **Análise do Resultado:** A saída confirma que o host analyst possui três interfaces de rede, cada uma com um IP numa das redes do escopo (10.10.10.x, 10.10.30.x, 10.10.50.x), validando a nossa capacidade de analisar todo o ambiente.
- **Comando Executado:** ip a | grep inet
- **Explicação do Comando:** O grep inet é usado para filtrar a saída longa do ip a, mostrando apenas as linhas que contêm os endereços IP (IPv4 e IPv6), tornando a visualização mais limpa.
- Resultado:



- **Análise do Resultado:** Este resultado limpo serve como uma referência rápida dos nossos pontos de acesso em cada sub-rede.
- **Comando Executado:** ip a | grep inet > recon-redes.txt

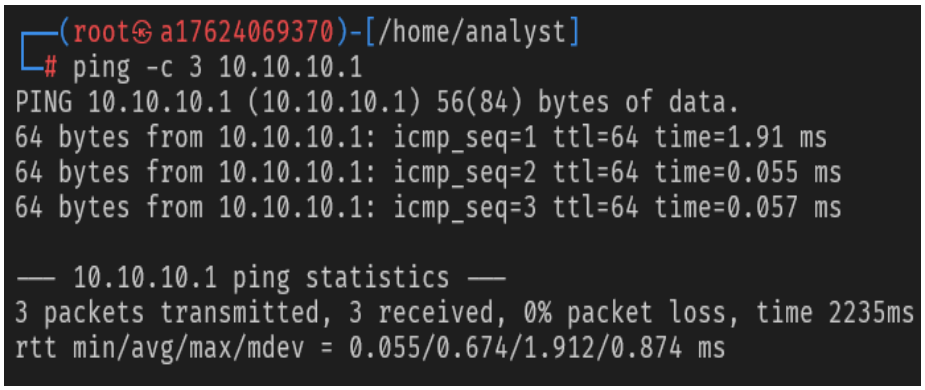
- **Explicação do Comando:** O > redireciona a saída do comando anterior para um ficheiro de texto, guardando a nossa primeira evidência de forma permanente.
- Resultado:



- **Análise do Resultado:** Este passo documenta a prática de guardar os resultados, garantindo que as evidências não se perdem.

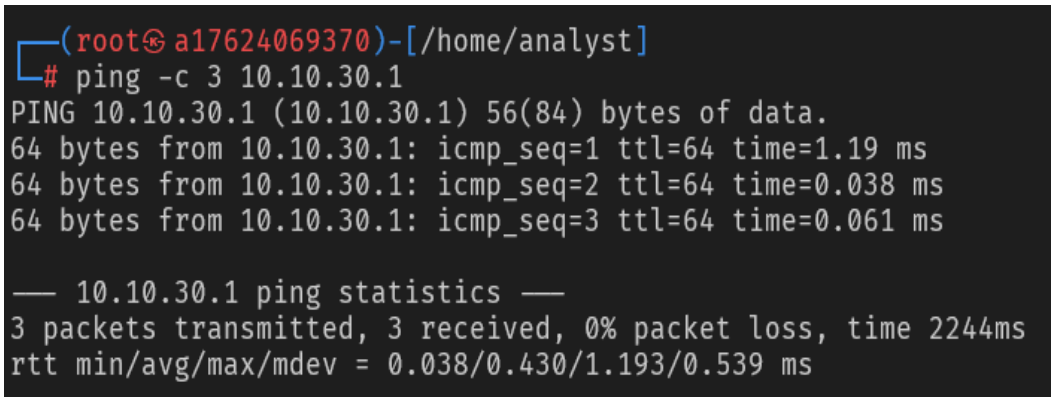
Anexo B: Teste de Conectividade com as Redes

- **Comando Executado:** ping -c 3 10.10.10.1
- **Explicação do Comando:** O ping -c 3 envia três pacotes ICMP para um alvo para verificar se há comunicação. É o teste mais básico para confirmar que conseguimos "alcançar" as outras redes.
- Resultado:

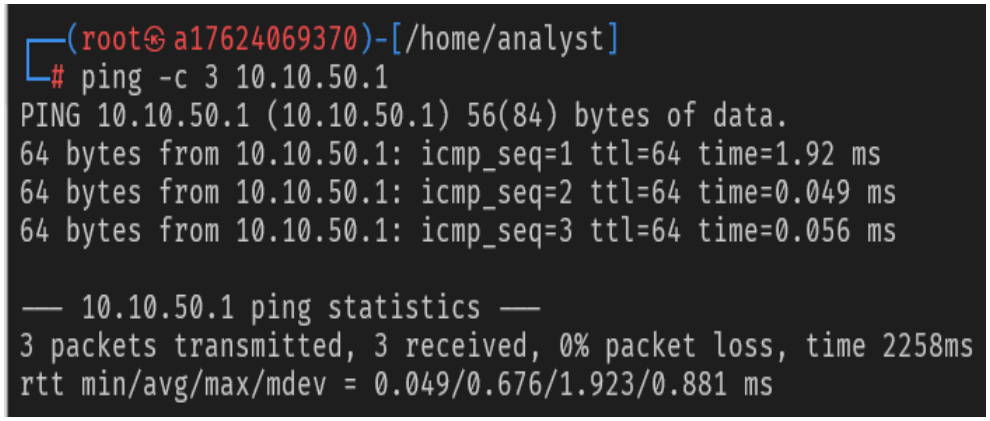


- **Análise do Resultado:** A resposta com 0% packet loss confirma que a comunicação com a rede corp_net está a funcionar.
- **Comando Executado:** ping -c 3 10.10.30.1
- **Explicação do Comando:** O mesmo teste de ping é realizado para a rede guest_net.

- Resultado:



- **Análise do Resultado:** A resposta positiva confirma a comunicação com a rede guest_net.
- **Comando Executado:** ping -c 3 10.10.50.1
- **Explicação do Comando:** O mesmo teste de ping é realizado para a rede infra_net.
- Resultado:



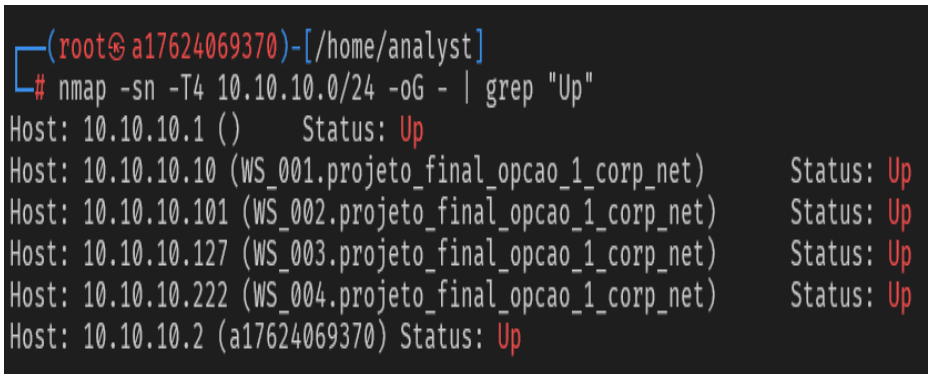
- **Análise do Resultado:** A resposta positiva confirma a comunicação com a rede infra_net.

Fase 2: Descoberta de Ativos

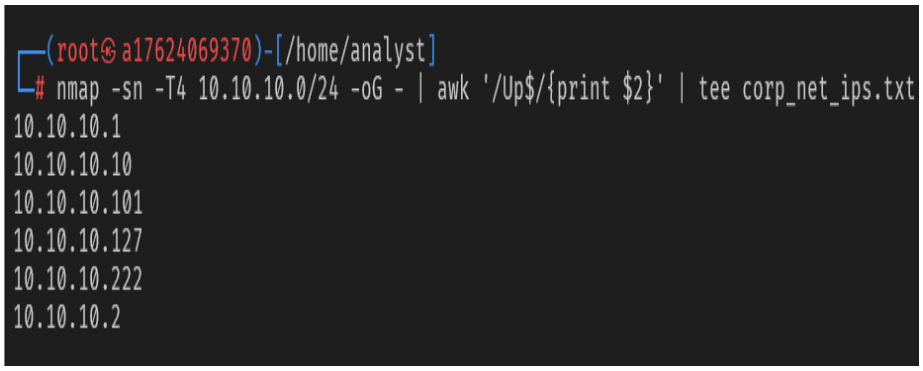
Anexo C: Descoberta de Hosts na corp_net **(10.10.10.0/24)**

- **Comando Executado:** nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
- **Explicação do Comando:** O nmap -sn (Ping Scan) varre uma gama de IPs para ver quem responde, descobrindo hosts ativos. O -oG - | grep "Up" formata a saída para ser fácil de ler, mostrando apenas os hosts que estão "Up" (ligados).

- Resultado:



- **Análise do Resultado:** A saída lista todos os IPs e hostnames dos computadores que estão ligados na rede corp_net, formando a base do nosso inventário.
- **Comando Executado:** nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2}' | tee corp_net_ips.txt
- **Explicação do Comando:** O awk '/Up$/{print $2}' processa a saída do Nmap para extrair apenas a segunda coluna (o endereço IP) de cada host ativo. O tee mostra o resultado no ecrã e guarda-o no ficheiro corp_net_ips.txt.
- Resultado:



- **Análise do Resultado:** Este comando cria uma lista de alvos limpa, contendo apenas os IPs dos hosts ativos, que será usada nos próximos scans.
- **Comando Executado:** nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee corp_net_ips_hosts.txt
- **Explicação do Comando:** Semelhante ao anterior, mas o print $2, $3 extrai tanto o IP como o hostname, criando um ficheiro de inventário rápido.

- Resultado:

```
┌──(root㉿a17624069370)-[/home/analyst]
└─# nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee corp_net_ips_hosts.txt
10.10.10.1 ()
10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net)
10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net)
10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net)
10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net)
10.10.10.2 (a17624069370)
```

- **Análise do Resultado:** Este ficheiro serve como uma referência rápida para associar IPs a nomes de máquinas.

Anexo D: Descoberta de Hosts na guest_net **(10.10.30.0/24)**

- **Comando Executado:** nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
- **Explicação do Comando:** Repetição do processo de descoberta para a rede de visitantes/servidores.
- Resultado:

```
┌──(root㉿a17624069370)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
Host: 10.10.30.1 ()     Status: Up
Host: 10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net)  Status: Up
Host: 10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net)        Status: Up
Host: 10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net)        Status: Up
Host: 10.10.30.17 (openldap.projeto_final_opcao_1_infra_net)    Status: Up
Host: 10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net)      Status: Up
Host: 10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)      Status: Up
Host: 10.10.30.2 (a17624069370) Status: Up
```

- **Análise do Resultado:** A saída lista todos os servidores críticos que estão incorretamente localizados nesta rede.
- **Comando Executado:** nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2}' | tee infra_net_ips.txt
- **Explicação do Comando:** Extração da lista de IPs dos servidores.

- Resultado:

```
┌──(root㉿a17624069370)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2}' | tee infra_net_ips.txt
10.10.30.1
10.10.30.10
10.10.30.11
10.10.30.15
10.10.30.17
10.10.30.117
10.10.30.227
10.10.30.2
```

- **Análise do Resultado:** Cria a lista de alvos para a análise aprofundada dos servidores.
- **Comando Executado:** nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee infra_net_ips_hosts.txt
- **Explicação do Comando:** Extração dos IPs e hostnames dos servidores.
- Resultado:

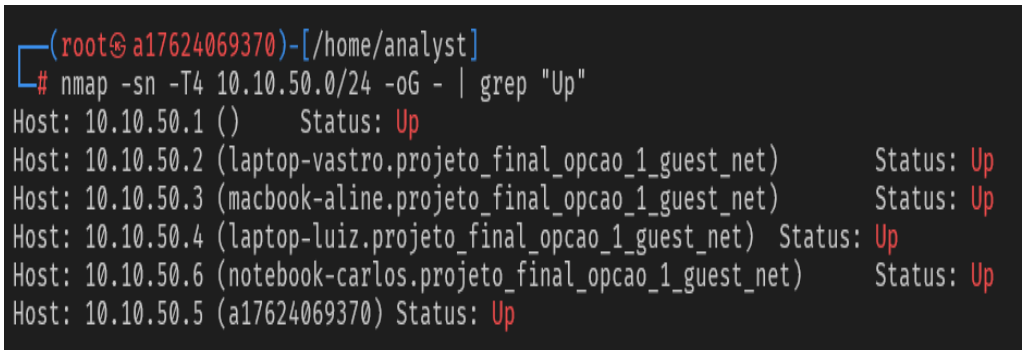
```
┌──(root㉿a17624069370)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee infra_net_ips_hosts.txt
10.10.30.1 ()
10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net)
10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net)
10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net)
10.10.30.17 (openldap.projeto_final_opcao_1_infra_net)
10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net)
10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)
10.10.30.2 (a17624069370)
```

- **Análise do Resultado:** Cria o ficheiro de inventário para a rede de servidores.

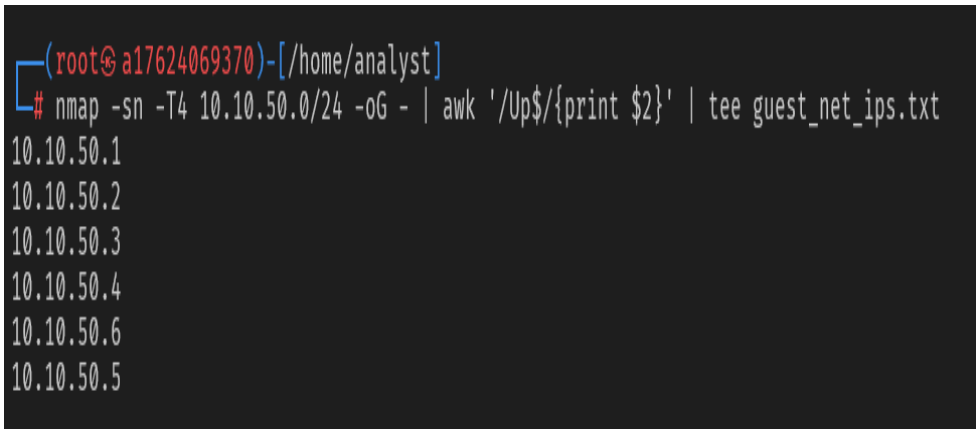
Anexo E: Descoberta de Hosts na infra_net (10.10.50.0/24)

- **Comando Executado:** nmap -sn -T4 10.10.50.0/24 -oG - | grep "Up"
- **Explicação do Comando:** Repetição do processo de descoberta para a rede de infraestrutura/utilizadores.

- Resultado:



- **Análise do Resultado:** A saída mostra que esta rede contém apenas dispositivos de utilizadores finais, confirmando a falha de segmentação.
- **Comando Executado:** nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2}' | tee guest_net_ips.txt
- **Explicação do Comando:** Extração da lista de IPs dos dispositivos de utilizadores.
- Resultado:



- **Análise do Resultado:** Cria a lista de alvos para a verificação de portas nos dispositivos dos utilizadores.
- **Comando Executado:** nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee guest_net_ips_hosts.txt
- **Explicação do Comando:** Extração dos IPs e hostnames dos dispositivos dos utilizadores.

- Resultado:

```
┌──(root㉿a17624069370)-[/home/analyst]
└─# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee guest_net_ips_hosts.txt
10.10.50.1 ()
10.10.50.2 (laptop-vastro.projeto_final_opcao_1_guest_net)
10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net)
10.10.50.4 (laptop-luiz.projeto_final_opcao_1_guest_net)
10.10.50.6 (notebook-carlos.projeto_final_opcao_1_guest_net)
10.10.50.5 (a17624069370)
```

- **Análise do Resultado:** Cria o ficheiro de inventário para a rede de utilizadores.

Fase 3: Escaneamento de Portas

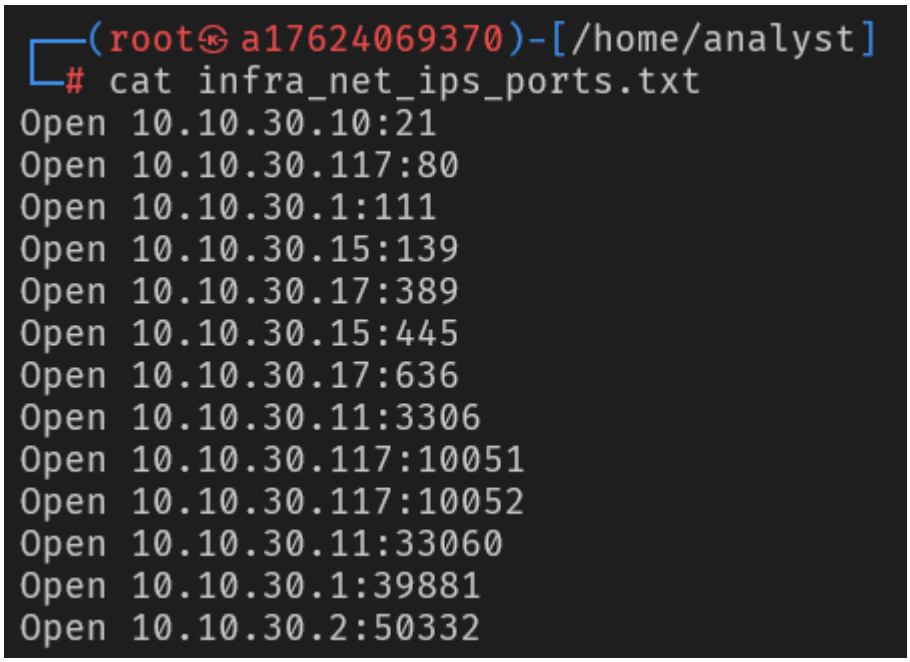
Anexo F: Lista Rápida de Portas Abertas

- **Comando Executado:** rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt
- **Explicação do Comando:** O rustscan é usado para uma varredura muito rápida de portas em todos os hosts da lista. O grep Open filtra apenas as portas abertas e o > guarda o resultado num ficheiro.
- Resultado:

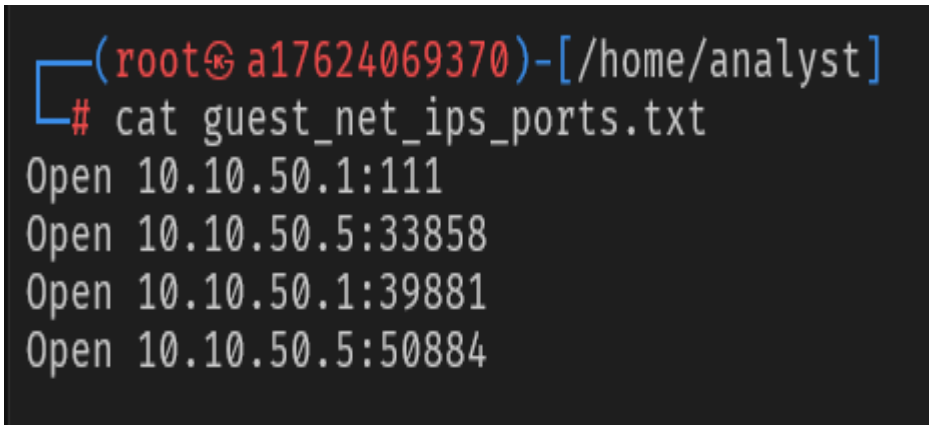
```
┌──(root㉿a17624069370)-[/home/analyst]
└─# cat corp_net_ips_ports.txt
Open 10.10.10.1:111
Open 10.10.10.1:39881
```

- **Análise do Resultado:** A saída fornece uma lista rápida de todos os IPs e as suas respetivas portas abertas na rede corp_net.
- **Comando Executado:** rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt
- **Explicação do Comando:** Repetição da varredura rápida de portas para a rede de servidores.

- Resultado:



- **Análise do Resultado:** A saída mostra uma grande quantidade de portas abertas, correspondendo aos vários serviços de servidor.
- **Comando Executado:** rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt
- **Explicação do Comando:** Repetição da varredura rápida de portas para a rede de utilizadores.
- Resultado:

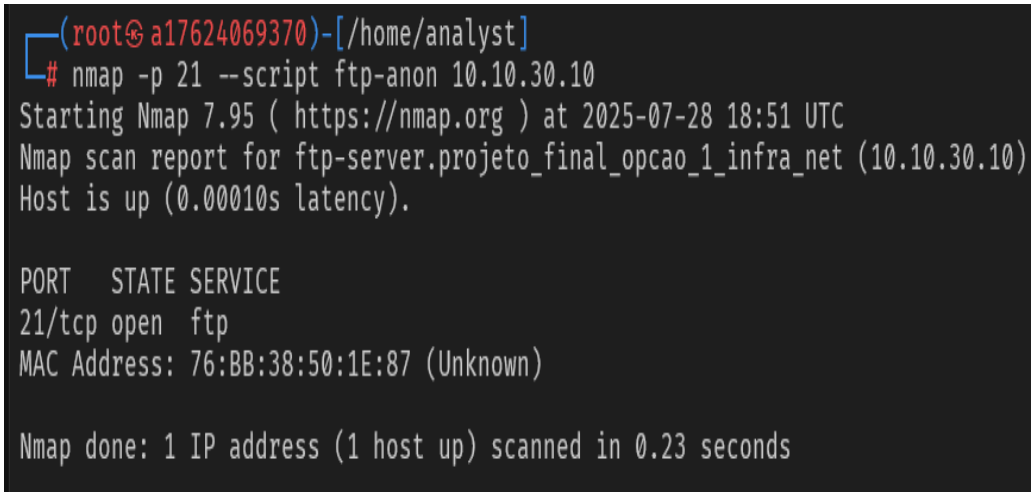


- **Análise do Resultado:** A saída mostra muito poucas portas abertas, o que é esperado e positivo para dispositivos de utilizadores finais.

Fase 4: Análise Aprofundada de Serviços

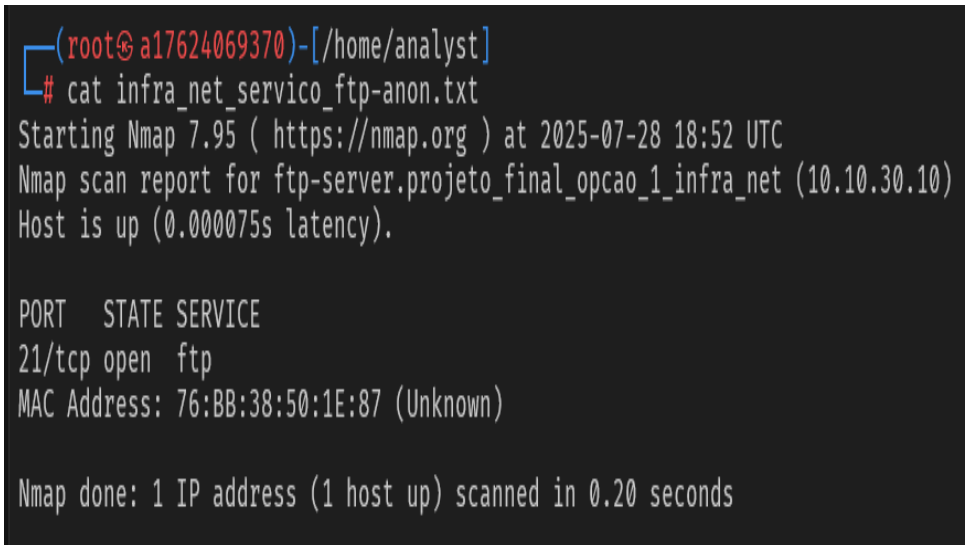
Anexo G: Investigação do Serviço FTP (10.10.30.10)

- **Comando Executado:** nmap -p 21 --script ftp-anon 10.10.30.10
- **Explicação do Comando:** O script --script ftp-anon do Nmap tenta autenticar-se no servidor FTP com o utilizador "anonymous". É um teste direto para uma das configurações erradas mais comuns e perigosas.
- Resultado:



- **Análise do Resultado:** A ausência da mensagem "Anonymous FTP login allowed" na saída significa que o servidor está corretamente configurado para não permitir este tipo de acesso, o que é um ponto positivo de segurança.
- **Comando Executado:** nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt
- **Explicação do Comando:** Este comando executa o mesmo teste, mas guarda a saída diretamente num ficheiro para documentação.

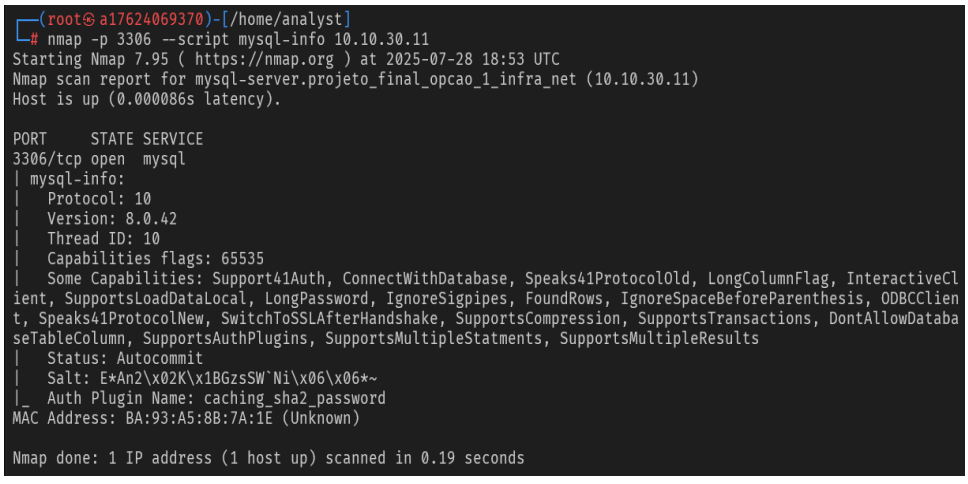
- Resultado:



- **Análise do Resultado:** Documenta a criação da evidência.

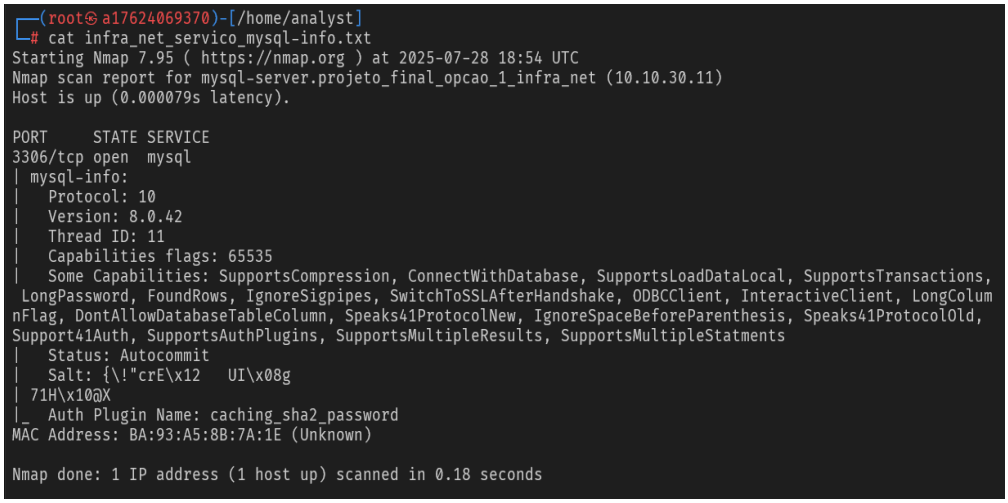
Anexo H: Investigação do Serviço MySQL (10.10.30.11)

- **Comando Executado:** nmap -p 3306 --script mysql-info 10.10.30.11
- **Explicação do Comando:** O script mysql-info tenta obter informações do serviço MySQL sem precisar de se autenticar.
- Resultado:



- **Análise do Resultado:** A saída mostra que o servidor vaza informações detalhadas da versão (8.0.42) e do método de autenticação, o que é uma fuga de informação valiosa para um atacante.
- **Comando Executado:** nmap -p 3306 --script mysql-info 10.10.30.11 > infra_net_servico_mysql-info.txt

- **Explicação do Comando:** Guarda o resultado da investigação do MySQL num ficheiro.
- Resultado:



- **Análise do Resultado:** Documenta a criação da evidência.

Anexo I: Investigação do Serviço LDAP (10.10.30.17)

- **Comando Executado:** nmap -p 389 --script ldap-rootdse 10.10.30.17
- **Explicação do Comando:** O script ldap-rootdse tenta obter a "base" de informações de um servidor LDAP sem autenticação.

- Resultado:

```
┌──(root㉿a17624069370)-[/home/analyst]
└─# nmap -p 389 --script ldap-rootdse 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 18:55 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.00012s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       namingContexts: dc=example,dc=org
|       supportedControl: 2.16.840.1.113730.3.4.18
|       supportedControl: 2.16.840.1.113730.3.4.2
|       supportedControl: 1.3.6.1.4.1.4203.1.10.1
|       supportedControl: 1.3.6.1.1.22
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.826.0.1.3344810.2.3
|       supportedControl: 1.3.6.1.1.13.2
|       supportedControl: 1.3.6.1.1.13.1
|       supportedControl: 1.3.6.1.1.12
|       supportedExtension: 1.3.6.1.4.1.1466.20037
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.1
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.3
|       supportedExtension: 1.3.6.1.1.8
|       supportedLDAPVersion: 3
|       supportedSASLMechanisms: SCRAM-SHA-1
|       supportedSASLMechanisms: SCRAM-SHA-256
|       supportedSASLMechanisms: GS2-IAKERB
|       supportedSASLMechanisms: GS2-KRB5
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedSASLMechanisms: OTP
|       supportedSASLMechanisms: CRAM-MD5
|       supportedSASLMechanisms: NTLM
|_      subschemaSubentry: cn=Subschema
MAC Address: BE:04:FF:EC:24:53 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

- **Análise do Resultado:** A saída confirma a falha crítica. O servidor responde a conexões anónimas e revela o namingContext (dc=example,dc=org), permitindo a um atacante mapear toda a estrutura de utilizadores.
- **Comando Executado:** nmap -p 389 --script ldap-rootdse 10.10.30.17 > infra_net_servico_ldap-rootdse.txt
- **Explicação do Comando:** Guarda o resultado da investigação do LDAP num ficheiro.

- Resultado:

```
┌──(root㉿a17624069370)-[/home/analyst]
└─# cat infra_net_servico_ldap-rootdse.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 18:56 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000090s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       namingContexts: dc=example,dc=org
|       supportedControl: 2.16.840.1.113730.3.4.18
|       supportedControl: 2.16.840.1.113730.3.4.2
|       supportedControl: 1.3.6.1.4.1.4203.1.10.1
|       supportedControl: 1.3.6.1.1.22
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.826.0.1.3344810.2.3
|       supportedControl: 1.3.6.1.1.13.2
|       supportedControl: 1.3.6.1.1.13.1
|       supportedControl: 1.3.6.1.1.12
|       supportedExtension: 1.3.6.1.4.1.1466.20037
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.1
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.3
|       supportedExtension: 1.3.6.1.1.8
|       supportedLDAPVersion: 3
|       supportedSASLMechanisms: SCRAM-SHA-1
|       supportedSASLMechanisms: SCRAM-SHA-256
|       supportedSASLMechanisms: GS2-IAKERB
|       supportedSASLMechanisms: GS2-KRB5
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedSASLMechanisms: OTP
|       supportedSASLMechanisms: CRAM-MD5
|       supportedSASLMechanisms: NTLM
|_      subschemaSubentry: cn=Subschema
MAC Address: BE:04:FF:EC:24:53 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

- **Análise do Resultado:** Documenta a criação da evidência.

Anexo J: Investigação do Serviço Samba (10.10.30.15)

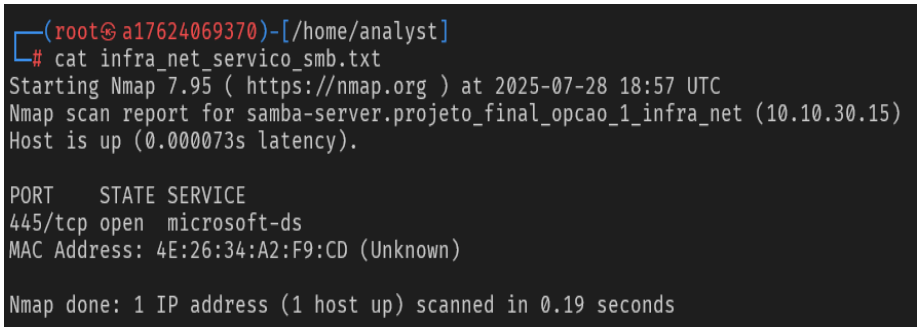
- **Comando Executado:** nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
- **Explicação do Comando:** O Nmap usa dois scripts: smb-os-discovery para tentar adivinhar o sistema operativo e smb-enum-shares para tentar listar partilhas de ficheiros abertas.
- Resultado:

```
┌──(root㉿a17624069370)-[/home/analyst]
└─# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 18:57 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000087s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 4E:26:34:A2:F9:CD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

- **Análise do Resultado:** A saída mostra que o servidor está a correr Samba, mas não lista nenhuma partilha, indicando que a enumeração anónima está corretamente desativada.
- **Comando Executado:** nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15 > infra_net_servico_smb.txt
- **Explicação do Comando:** Guarda o resultado da investigação do Samba num ficheiro.
- Resultado:



- **Análise do Resultado:** Documenta a criação da evidência.

Anexo K: Investigação do Serviço HTTP (10.10.30.117)

- **Comando Executado:** curl -I http://10.10.30.117
- **Explicação do Comando:** O curl -I obtém apenas os cabeçalhos (headers) de uma página web, sem descarregar o conteúdo. É útil para ver rapidamente informações do servidor.

- Resultado:

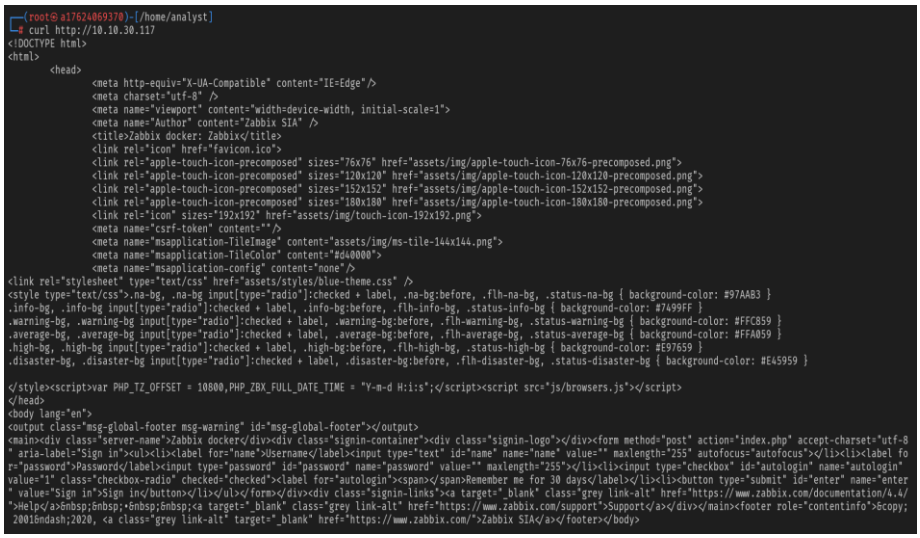
```
┌──(root㉿a17624069370)-[/home/analyst]
└─# curl -I http://10.10.30.117
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 28 Jul 2025 18:59:17 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Keep-Alive: timeout=20
X-Powered-By: PHP/7.3.14
Set-Cookie: PHPSESSID=d17c4541a519265cee2c4ea45149064e; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
```

- **Análise do Resultado:** A saída revela o tipo de servidor (nginx) e, mais importante, a versão exata do PHP (7.3.14), o que é uma fuga de informação.
- **Comando Executado:** curl -I http://10.10.30.117 > infra_net_servico_webserver.txt
- **Explicação do Comando:** Guarda os cabeçalhos HTTP num ficheiro.
- Resultado:

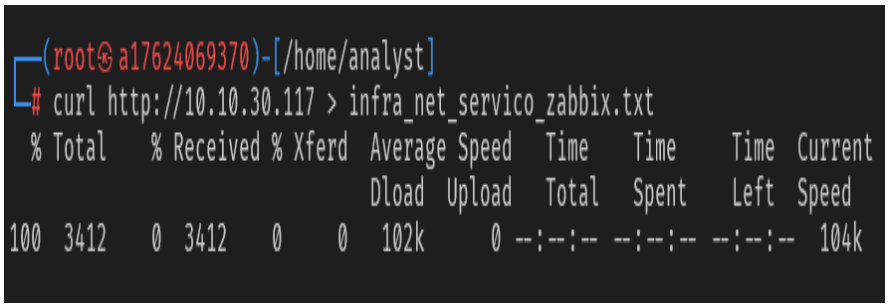
```
┌──(root㉿a17624069370)-[/home/analyst]
└─# curl -I http://10.10.30.117 > infra_net_servico_webserver.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

- **Análise do Resultado:** Documenta a criação da evidência.
- **Comando Executado:** curl http://10.10.30.117
- **Explicação do Comando:** Este comando descarrega e mostra o código-fonte HTML completo da página.

- Resultado:



- **Análise do Resultado:** A análise do código HTML pode revelar mais informações, como comentários, links para outros ficheiros ou nomes de utilizador.
- **Comando Executado:** curl http://10.10.30.117 > infra_net_servico_zabbix.txt
- **Explicação do Comando:** Guarda o código-fonte HTML da página num ficheiro.
- Resultado:



- **Análise do Resultado:** Documenta a criação da evidência.